



FEE TRANSMITTAL FOR FY 2007

(FY 2005 Begins 10/01/2004. Fee changes made on 11/22/04 and 12/08/04 are included.)

TOTAL AMOUNT OF PAYMENT (\$) **250.00**

Complete if Known:

Application No. 09/707,417
 Filing Date November 6, 2000
 First Named Inventor Vance C. Bjorn
 Examiner Name Moorthy, Aravind K.
 Art Unit 2131
 Attorney Docket No. 003022.P019X

Applicant claims small entity status. See 37 CFR 1.27.

METHOD OF PAYMENT (check all that apply)

Check Credit Card Money Order Other None
 Deposit Account

Deposit Account Number : 02-2666

Deposit Account Name: _____

The Director is Authorized to do the following with respect to the above-identified Deposit Account:

- Charge fee(s) indicated below.
- Credit any overpayments.
- Charge any additional fees during the pendency of this application.
- Any concurrent or future reply that requires a petition for extension of time should be treated as incorporating an appropriate petition for extension of time and all required fees should be charged.
- Charge fee(s) indicated below except for the filing fee

FEE CALCULATION

1A. BASIC FILING FEE/SEARCH FEE/EXAMINATION FEE

<u>Large Entity</u>		<u>Small Entity</u>		<u>Fee Description</u>		<u>Fee Paid</u>
Fee	Fee	Fee	Fee			
Code	(\$)	Code	(\$)	Utility application filing fee		\$
1011	300	2011	150		1,000/500*	
1111	500	2111	250	Utility search fee		\$
1311	200	2311	100	Utility examination fee		\$
1012	200	2012	100	Design application filing fee	430/215*	
1112	100	2112	50	Design search fee		
1312	130	2312	65	Design examination fee		
1013	200	2013	100	Plant filing fee	660/330*	
1113	300	2113	150	Plant search fee		
1313	160	2313	80	Plant examination fee		
1004	300	2004	150	Reissue filing fee	1,400/700*	
1114	500	2114	250	Reissue search fee		
1314	600	2314	300	Reissue examination fee		
1005	200	2005	100	Provisional application filing fee		

SUBTOTAL (1) \$ 0.00

* List the filing, search, and examination fees separately, but pay concurrently.

1B. APPLICATION SIZE FEE

				<u>Extra Sheets</u>	<u>Fee from below</u>	<u>Fee paid</u>
Total Sheets _____ - 100 =				/50 = _____ * X \$125.00		
*(round up to integer)						
<u>Large Entity</u>	<u>Small Entity</u>					
Fee Code	Fee (\$)	Fee Code	Fee (\$)	<u>Fee Description</u>		
1081	250	2081	125	Utility application size fee for each additional group of 50 sheets beyond initial 100 sheets (count spec & drawings except sequences & program listings)		
1082	250	2082	125	Design application size fee for each additional group of 50 sheets beyond initial 100 sheets (count spec & drawings except sequences & program listings)		
1083	250	2083	125	Plant application size fee for each additional group of 50 sheets beyond initial 100 sheets (count spec & drawings except sequences & program listings)		
1084	250	2084	125	Reissue application fee for each additional group of 50 sheets beyond initial 100 sheets (count spec & drawings except sequences & program listings)		
SUBTOTAL (2) \$ _____						

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

				<u>Extra Claims</u>	<u>Fee from below</u>	<u>Fee Paid</u>
Total Claims _____ - 20** = _____				X \$25.00	= _____	
Independent Claims _____ - 3** = _____				X \$100.00	= _____	
Multiple Dependent				_____	= _____	
**Or number previously paid, if greater; For Reissues, see below.						
<u>Large Entity</u>	<u>Small Entity</u>	<u>Fee</u>	<u>Fee</u>	<u>Fee</u>	<u>Fee</u>	
Code	(\$)	Code	(\$)	<u>Fee Description</u>		
1202	50	2202	25	Claims in excess of 20		
1201	200	2201	100	Independent claims in excess of 3		
1203	360	2203	180	Multiple dependent claim, if not paid		
1204	200	2204	100	**Reissue independent claims over original patent		
1205	50	2205	25	**Reissue claims in excess of 20 and over original patent		
SUBTOTAL (3) \$ 0.00						

FEE CALCULATION (continued)

3. ADDITIONAL FEES

<u>Large Entity</u>		<u>Small Entity</u>		
Fee	Fee	Fee	Fee	
Code	(\$)	Code	(\$)	<u>Fee Description</u>
1051	130	2051	65	Surcharge - late filing fee or oath
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet
1053	130	1053	130	Non-English specification
1812	2,520	1812	2,520	For filing a request for ex parte reexamination
1813	8,800	1813	8,800	Request for inter parties reexamination
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action
1251	120	2251	60	Extension for reply within first month
1252	450	2252	225	Extension for reply within second month
1253	1,020	2253	510	Extension for reply within third month
1254	1,590	2254	795	Extension for reply within fourth month
1255	2,160	2255	1,080	Extension for reply within fifth month
1401	500	2401	250	Notice of Appeal
1402	500	2402	250	Filing a brief in support of an appeal
1403	1,000	2403	500	Request for oral hearing
1451	1,510	1451	1,510	Petition to institute a public use proceeding
1452	500	2452	250	Petition to revive – unavoidable
1453	1,500	2453	750	Petition to revive - unintentional
1501	1,400	2501	700	Utility issue fee (or reissue)
1502	800	2502	400	Design issue fee
1503	1100	2503	550	Plant issue fee
1464	130	1460	130	Petitions to the Commissioner (CFR 1.17(h) Group III)
1463	200	1460	200	Petitions to the Commissioner (CFR 1.17(g) Group II)
1462	400	1460	400	Petitions to the Commissioner (CFR 1.17(f) Group I)
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)
1806	180	1806	180	Submission of Information Disclosure Stmt
8021	40	8021	40	Recording each patent assignment per property (times number of properties)
1809	790	2809	395	For filing a submission after final rejection (see 37 CFR 1.129(a))
1814	130	2814	65	Statutory Disclaimer
1810	790	2810	395	For each additional invention to be examined (see 37 CFR 1.129(b))
1801	790	2801	395	Request for Continued Examination (RCE)
1802	900	1802	900	Request for expedited examination of a design application
1504	300	1504	300	Publication fee for early, voluntary, or normal pub.
1505	300	1505	300	Publication fee for republication
1803	130	1803	130	Request for voluntary publication or republication
1808	130	1808	130	Processing fee under 37 CFR 1.17(i) (except provisionals)
1454	1,370	1454	1,370	Acceptance of unintentionally delayed claim for priority

Other fee (specify) _____

Other fee (specify) _____

SUBTOTAL (4) \$ 250.00

*Reduced by Basic Filing Fee Paid

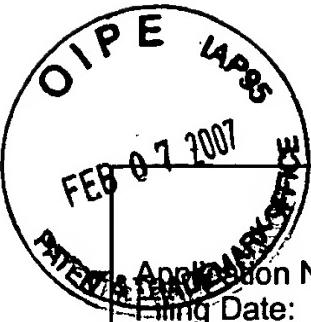
SUBMITTED BY:

Typed or Printed Name: Benjamin A. Kimes

Signature:  Date: February 5, 2007

Reg. Number: 50,870 Telephone Number: 408-720-8300

Send to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450



AF/2131

TRANSMITTAL LETTERPATENT

Application No.: 09/707,417
Filing Date: November 6, 2000
First Named Inventor Vance C. Bjorn
Examiner's Name: Moorthy, Aravind K.
Art Unit: 2131
Attorney Docket No.: 003022.P019X

- An Amendment After Final Action (37 CFR 1.116) is attached and applicant(s) request expedited action.
 Charge any fee not covered by any check submitted to Deposit Account No. 02-2666.
 Applicant(s) hereby request and authorize the U.S. Patent and Trademark Office to (1) treat any concurrent or future reply that requires a petition for extension of time as incorporating a petition for extension of time for the appropriate length of time and (2) charge all required fees, including extension of time fees and fees under 37 CFR 1.16 and 1.17, for any concurrent or future reply to Deposit Account No. 02-2666.
 Applicant(s) claim small entity status (37 CFR 1.27).

ATTACHMENTS

- Preliminary Amendment
 Amendment/Response with respect to Office Action
 Amendment/Response After Final Action (37 CFR 1.116) (reminder: consider filing a Notice of Appeal)
 Notice of Appeal
 RCE (Request for Continued Examination)
 Supplemental Declaration
 Terminal Disclaimer (reminder: if executed by an attorney, the attorney must be properly of record)
 Information Disclosure Statement (IDS)
 Copies of IDS citations
 Petition for Extension of Time
 Fee Transmittal Document (that includes a fee calculation based on the type and number of claims)
 Cross-Reference to Related Application(s)
 Certified Copy of Priority Document
 Other: Appeal Brief (29 pages)
 Other: Deposit Account Authorization for fees
 Check(s) _____
 Postcard (Return Receipt)

SUBMITTED BY:

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP

TYPED OR PRINTED NAME: Benjamin A. Kimes

SIGNATURE:

REG. NO.: 50,870DATE: February 5, 2007ADDRESS: 12400 Wilshire Boulevard, Seventh FloorLos Angeles, California 90030TELEPHONE NO.: (408) 720-8300CERTIFICATE OF MAILING BY FIRST CLASS MAIL (if applicable)

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to Mail Stop Appeal Brief- Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on February 5, 2007

Date of Deposit
Dianne Neathery

Dianne Neathery
Signature

Name of Person Mailing Correspondence

February 5, 2007

Date

Express Mail Label No. (if applicable): _____

(10/14/03)

Send to: COMMISSIONER FOR PATENTS, P.O. Box 1450, Alexandria, Virginia 22313-1450



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In Re Application of:

Vance C. Bjorn

Application No.: 09/707,417

Filed: November 6, 2000

For: A METHOD AND APPARATUS FOR
USING A THIRD PARTY
AUTHENTICATION SERVER

Examiner: Aravind K. Moorthy

Art Unit: 2131

Confirmation Number: 9958

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.
on <u>February 5, 2007</u>
Date of Deposit

Dianne Neathery
Name of Person Mailing Correspondence

<u>Dianne Neathery</u>	2/5/07
Signature	Date

Mail Stop Appeal Brief- Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Pursuant to 37 C.F.R. § 1.192, Appellants submit the following Appeal Brief for consideration by the Board of Patent Appeals and Interferences (hereinafter "Board"). Appellants also submit herewith a check in the amount of \$250.00 to cover the cost of filing this opening brief, as set forth in 37 C.F.R. § 1.17(c). Please charge any additional amounts due or credit any overpayment to Deposit Account No. 02-2666.

02/07/2007 MWOLGE1 00000005 022666 09707417

01 FC:2402 250.00 DA

TABLE OF CONTENTS

I.	Real Party in Interest	5
II.	Related Appeals and Interferences.....	5
III.	Status of Claims.....	5
IV.	Status of Amendments.....	5
V.	Summary of The Claimed Subject Matter	5
VI.	Grounds of Rejection To be Reviewed on Appeal	10
VII.	Argument	11
A.	Claims 1-6, 8, 9, and 11-14, 17, 20, 21, 23, 24, 26, 27 and 29-31 are not anticipated by U.S. Patent No. 6,594,376 B2 to Hoffman et al ("Hoffman) because Hoffman fails to teach or suggest each of the elements	11
1.	Claim 1 and associated dependent claims 2-6, 8, 9 and 11-13 are not anticipated by Hoffman because Hoffman fails to teach or suggest receiving a record ID for a user.....	11
2.	Claim 14 is not anticipated by Hoffman because Hoffman fails to teach or suggest looking up a record ID associated with a user.	13
3.	Claim 17 and associated dependent claims 20, 21, 23, 24, 26, 27 and 29-31 are not anticipated by Hoffman because Hoffman does not teach or suggest an authentication server to receive a record ID for a user.....	13
B.	Claims 7, 10, 25 and 28 are not obvious under 35 U.S.C. §103(a) in view of Hoffman and U.S. Patent No. 6,581,161 B1 to Byford ("Byford") because neither Hoffman nor Byford, alone or in combination, teach or suggest all of the elements.....	14

1.	Claim 7 is not obvious under 35 U.S.C. §103(a) in view of Hoffman and Byford because neither Hoffman nor Byford, alone or in combination, teach or suggest receiving a record ID for a user.....	14
2.	Claim 10 is not obvious under 35 U.S.C. §103(a) in view of Hoffman and Byford because neither Hoffman nor Byford, alone or in combination, teach or suggest discarding a record ID after returning a one-time key to the user.....	15
3.	Claim 25 is not obvious under 35 U.S.C. §103(a) in view of Hoffman and Byford because neither Hoffman nor Byford, alone or in combination, teach or suggest an authentication server to receive a record ID for a user.....	16
4.	Claim 28 is not obvious under 35 U.S.C. §103(a) in view of Hoffman and Byford because neither Hoffman nor Byford, alone or in combination, teach or suggest a security mechanism to discard the record ID after returning the one-time key to the user.....	17
C.	Claims 15, 16, 18 and 21 are not obvious under 35 U.S.C. §103(a) in view of Hoffman and U.S. Patent No. 5,692,106 to Towers et al ("Towers") because neither Hoffman nor Towers, alone or in combination, teaches or suggests each of the elements.....	18
1.	Claims 15 and 16 are not obvious under 35 U.S.C. §103(a) in view of Hoffman and Towers because neither Hoffman nor Towers, alone or in combination, teach or suggest looking up a record ID associated with a user.....	18

2. Claims 18 and 21 are not obvious under 35 U.S.C. §103(a) in view of Hoffman and Towers because neither Hoffman nor Towers, alone or in combination, teach or suggest an authentication server to receive a record ID for a user.....	19
D. Claims 19 and 22 are not obvious under 35 U.S.C. §103(a) in view of Hoffman and U.S. Patent No. 6,119,227 to Mao ("Mao") because neither Hoffman nor Mao, alone or in combination, teach or suggest a server to receive a record ID for a user.....	19
VIII. Conclusion	21
IX. Claims Appendix	22
X. Evidence Appendix	28
XI. Related Proceedings Appendix.....	29

I. REAL PARTY IN INTEREST

The real party in interest is the assignee of the full interest in the invention, DigitalPersona, Inc., of 805 Veterans Boulevard, Suite 301, Redwood City, CA 94063.

II. RELATED APPEALS AND INTERFERENCES

To the best of Appellants' knowledge, there are no appeals or interferences related to the present appeal that will directly affect, be directly affected by, or have a bearing on the Board's decision in the instant appeal.

III. STATUS OF CLAIMS

Claims 1-31 are currently pending in the above-referenced application. Claims 1-31 were rejected in the Final Office Action mailed on June 17, 2004, and are presented for appeal. A copy of claims 1-31 as they stand on appeal are set forth in Appendix A.

IV. STATUS OF AMENDMENTS

No amendments were filed subsequent to the final rejection.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The instant application relates to a method and apparatus for providing a certificate from a client to a server. A request for a certificate is received from the server and forwarded to a biometric certification server (BCS). Biometric identification received by the server is forwarded to the BCS. If the biometric identification matches a registered user on the BCS, the client is identified to the server. (See Abstract).

Example implementations of independent claims 1, 14 and 17 are as follows. In independent claim 1, a method of authenticating a client, the method including an authentication server, includes receiving a record ID for a user. (Figure 5, block 525; Specification, page 10, lines 3-10; Figure 7, block 742, Specification, page 13, lines 5-11). The record ID is a random number generated for tracking authentication data and disassociating the authentication data from other client identity data. (Specification, page 10, lines 3-10). The method includes receiving a one-time key generated by a third party server and encrypted with a user's public key by the server. (Figure 7C, block 750; Specification, page 13, lines 19-22). The method includes receiving the user's authentication data from the client. (Figure 7C, block 742; Specification, page 13, lines 5-11). The method includes determining if the user's authentication data matches the record ID. (Figure 7C, block 744; Specification, page 13, lines 5-11). The method includes decrypting the one-time key with the user's private key and returning the decrypted one-time key if the user's authentication data matches the record ID. (Figure 7A, block 716, Specification, page 15, lines 4-7; Figure 9, block 960; Specification, page 16, lines 18-22 and page 17, lines 26-27).

In claim 7, the method notes that the authentication data is biometric data. (Figure 7C, block 744, Specification, page 13, lines 5-11).

Claim 10 recites that the method of authenticating a client further includes discarding the received record ID after returning the one-time key to the user. (Specification, page 15, lines 11-18).

In independent claim 14, Appellants claim a method of using an authentication server to authenticate a user to a third party server, the method including the third party

server looking up a record ID associated with the user. (Figure 5, block 525; Specification, page 10, lines 3-10; Figure 7A, block 703, Specification, page 12, lines 13-17). The record ID is a random number generated to track the user's authentication data and to separate the user's other identity information from the authentication data. (Specification, page 10, lines 3-10). The method includes generating a one-time key. (Figure 7C, block 750; Specification, page 13, lines 19-22). The method includes encrypting the one-time key with a public key of the user. (Figure 7C, block 752; Specification, page 13, lines 23-26). The method includes sending the encrypted one-time key and record ID to the user. (Figure 7C, block 754; Specification, page 13, lines 25-26). The method includes receiving the authentication data, the authentication data being the decrypted one-time key decrypted with the user's private key by the authentication server. (Figure 7A, block 716; Specification, page 15, lines 4-7). In the method, the user does not have control of the user's private key at any time. (Specification, page 18, lines 3-7). The method includes permitting access to the server. (Figure 7A, block 718; Specification, page 15, lines 4-7).

In claim 15, the method includes determining an authentication policy associated with the user. (Specification, page 8, lines 24-27; Figure 6, block 620; Specification, page 11, lines 18-20). In claim 15, the method includes verifying that the authentication policy has been satisfied, prior to access to the server. (Figure 7A, block 716, Specification, page 15, lines 4-7).

Claim 16 recites that in the method of using an authentication server to authenticate a user to a third party server, verifying that the authentication policy has been satisfied includes determining if the server should verify additional data.

(Specification, page 9, lines 20-27; page 13, lines 12-17). According to the method, if it is determined that the server should verify additional data, additional data is requested from the user. (Specification, page 13, lines 12-17). According to the method, the additional data is requested from the user prior to generation of the one-time password. (Figure 7C, block 750; Specification, page 13, lines 19-22).

In independent claim 17, Appellants claim a third-party authentication system that includes an authentication server to receive a record ID for a user. (Figure 2, block 250; Specification, page 5, lines 18-25). The record ID is a randomly generated number used to separate the user's authentication data and to separate the user's other identity information from the user's authentication data. (Specification, page 10, lines 3-10). The system includes a one-time key that is generated by a third party server and encrypted with a user's public key by the third party server. (Specification, page 5, lines 23-25). The system includes a comparison logic in the authentication server to receive the user authentication data from the client and determine whether the user's authentication data matches the record ID. (Figure 4, block 450; Specification, page 8, line 23 to page 9, line 3). The system includes a decryption logic in the authentication server to decrypt the one-time key with a private key associated with the validated record, and to return the decrypted one-time key to the client. (Figure 4, block 440; Specification, page 8, lines 11-22).

In claim 18, the system includes a policy validation logic to receive a policy from the third party server, and determine if the policy has been fulfilled. (Specification, page 7, lines 1-18). In claim 18, the system includes the decryption logic to decrypt the one-

time key only if the policy has been fulfilled. (Figure 4, block 440; Specification, page 8, lines 11-22).

Claim 19 recites that the system includes a nonce generation logic to generate a nonce, the nonce to be included with the user authentication data from the client. (Specification, page 8, lines 11-22). In the system, the comparison logic is to verify that the user authentication data includes the appropriate nonce. (Specification, page 8, line 22 to page 9, line 3).

Claim 21 recites that the system includes the interface to send the record ID and the public key to the user. (Figure 4, block 410; Specification, page 8, lines 11-14).

Claim 22 recites that in the system, the interface to establish a secure connection with the user, prior to receiving registration authentication data. (Figure 4, block 410; Specification, page 8, lines 11-14).

Claim 25 recites that in the system, the authentication data is biometric data. (Specification, page 7, lines 8-11).

Claim 28 recites that the system further includes a security mechanism to discard the received record ID after returning the one-time key to the user. (Figure 4, block 460; Specification, page 18, lines 17-21).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The issues involved in this Appeal are as follows:

- A. Whether claim 1-6, 8, 9, 11-14, 17, 20, 21, 23, 24, 26, 27 and 29-31 are anticipated by U.S. Patent No. 6,594,376 B2 to Hoffman et al ("Hoffman").
- B. Whether claims 7, 10, 25 and 28 are obvious under 35 U.S.C. §103(a) in view of Hoffman and U.S. Patent No. 6,581,161 B1 to Byford ("Byford").
- C. Whether claims 15, 16, 18 and 21 are obvious under 35 U.S.C. §103(a) in view of Hoffman and U.S. Patent No. 5,692,106 to Towers et al ("Towers").
- D. Whether claims 19 and 22 are obvious under 35 U.S.C. §103(a) in view of Hoffman and U.S. Patent No. 6,119,227 to Mao ("Mao").

VII. ARGUMENT

A. Claims 1-6, 8, 9, 11-14, 17, 20, 21, 23, 24, 26, 27 and 29-31 are not anticipated by U.S. Patent No. 6,594,376 B2 to Hoffman et al (“Hoffman) because Hoffman fails to teach or suggest each of the elements.

1. Claim 1 and associated dependent claims 2-6, 8, 9 and 11-13 are not anticipated by Hoffman because Hoffman fails to teach or suggest receiving a record ID for a user.

Appellants respectfully submit that Hoffman does not teach or suggest receiving a record ID for a user, much less a record ID being a random number generated for tracking authentication data and disassociating the authentication data from other client identity data.

Hoffman discloses the use of a PIN number, which is not the same as a record ID. The PIN number of Hoffman is part of the buyer's personal authentication information, which Hoffman explains comprises a PIN and at least one bid biometric sample. (Hoffman, Summary, column 4, lines 30-32). The PIN of Hoffman is used to search for the user in a particular bin of biometrics, thus in Hoffman it is expected that users will share the same PIN. (Hoffman, col. 9, line 65 to col. 10, line 4). The PIN is not used to for identifying a buyer's record, in contrast to a record ID. In fact, since Hoffman points out that the PIN is not unique, it cannot be used to identify a biometric record.

In Hoffman, authentication data is not disassociated from other client identity data. Hoffman discloses that the PIN is stored along with financial account numbers,

user name, and other user information on an individual biometric database (IDB).

(Hoffman, FIG. 10, col. 21, lines 29-41). Specifically, Hoffman states that:

Individual Biometric Database (IBD) records store personal information on buyers for both identification as well as authentication. This information includes their primary and secondary biometrics, one or more PIN codes, a list of financial accounts, account index codes, account index names, private code, one or more emergency account index codes, address, and phone number. The buyer may optionally include his SSN. This information is necessary for identifying a buyer either by biometric or personal information, for accessing related information, or for providing an address or phone number to remote sellers for additional verification.

(Hoffman, col. 33, lines 16-21).

Hoffman specifically **teaches away from dissociating biometric data from personally identifying data**, as indicated in the cited passage above. The PIN, biometric data, and personal data are all stored together. Therefore, the IDB is not an anonymous record, in which biometric data is not associated with identifying information. In Hoffman, if the IDB is compromised, a hacker will gain access to a buyer's name, address, biometric data, and possibly even social security number.

Claim 1 recites in part, "receiving a record ID for a user, the record ID being a random number generated for tracking authentication data and disassociating the authentication data from other client identity data," in contrast to Hoffman. As noted above, Hoffman specifically teaches away from a record ID being a random number used for tracking authentication data and for disassociating the authentication data from other client identity data. This is illustrated in Figure 10, which shows the elements of the biometric record in Hoffman, including a PIN that is linked to the biometric and/or address data. (Hoffman, Figure 10). Therefore, Hoffman does not teach or suggest disassociating the authentication data from other client identity data.

Accordingly, independent claim 1 and associated dependent claims 2-13, which include each and every limitation of claim 1, are not anticipated by Hoffman.

2. Claim 14 is not anticipated by Hoffman because Hoffman fails to teach or suggest looking up a record ID associated with a user.

Appellants respectfully submit that Hoffman does not teach or suggest looking up a record ID associated with the user, the record ID being a random number generated to track the user's authentication data and used to separate the user's other identity information from the authentication data, as recited in independent claim 14. As discussed above with reference to claim 1, Hoffman specifically teaches away from a record ID used to separate the user's other identity information from the authentication data.

Accordingly, independent claim 14 and associated dependent claims 15-16, which include each and every limitation of claim 14, are not anticipated by Hoffman.

3. Claim 17 and associated dependent claims 20, 21, 23, 24, 26, 27 and 29-31 are not anticipated by Hoffman because Hoffman does not teach or suggest an authentication server to receive a record ID for a user.

Appellants respectfully submit that Hoffman does not teach or suggest a server to receive a record ID for a user, as claimed in claim 17. Nor does Hoffman teach or suggest a record ID being a randomly generated number used to separate the user's other identity information from the user's authentication data. As discussed above with

reference to claim 1, Hoffman specifically teaches away from a record ID used to separate the user's other identity information from the authentication data.

Accordingly, independent claim 17 and associated dependent claims 18-31, which include each and every limitation of claim 17, are not anticipated by Hoffman.

B. Claims 7, 10, 25 and 28 are not obvious under 35 U.S.C. §103(a) in view of Hoffman and U.S. Patent No. 6,581,161 B1 to Byford (“Byford”) because neither Hoffman nor Byford, alone or in combination, teach or suggest all of the elements.

1. Claim 7 is not obvious under 35 U.S.C. §103(a) in view of Hoffman and Byford because neither Hoffman nor Byford, alone or in combination, teach or suggest receiving a record ID for a user.

Appellants respectfully submit that claim 7 is not obvious over the combination of Hoffman and Byford. Claim 7 depends on claim 1, and fully incorporates its limitations. Appellants respectfully submit that the combination of Hoffman and Byford does not teach or suggest receiving a record ID for a user, as claimed in claim 1.

Byford teaches the use of biometric data for authentication. However, Byford does not teach or suggest the use of a record ID in this context. As discussed above, Hoffman does not teach or suggest receiving a record ID for a user, and Byford does not supply the missing elements.

Since neither Hoffman nor Byford, alone or in combination, teaches receiving a record ID for a user as claimed in independent claim 1, the combination cannot be interpreted to render obvious Appellants' invention as claimed in associated claim 7.

Accordingly, Appellants respectfully request the withdrawal of the rejection over this combination.

2. Claim 10 is not obvious under 35 U.S.C. §103(a) in view of Hoffman and Byford because neither Hoffman nor Byford, alone or in combination, teach or suggest discarding a record ID after returning a one-time key to the user.

Appellants respectfully submit that claim 10 is not obvious over the combination of Hoffman and Byford. Claim 10 depends on claim 1, and incorporates all of its limitations, and therefore is patentable for at least the reasons discussed with reference to claim 1. Moreover, appellants respectfully submit that the combination of Hoffman and Byford does not teach or suggest discarding the record ID after returning the one-time key to the user, as claimed in claim 10.

The Examiner has admitted that Hoffman does not teach discarding the record ID after returning the one-time key to the user. (Office Action, 10/02/2006, page 8). The Examiner asserts that Byford teaches discarding the record ID, and asserts that the combination of Byford and Hoffman teach all of the limitations of claim 10.

Byford teaches the use of biometric data for authentication. However, Byford does not teach or suggest the use of a record ID in this context. As discussed above, Hoffman does not teach or suggest receiving a record ID for a user, and Byford does not supply the missing elements.

Byford does not teach a record ID, and therefore cannot teach discarding a user's record ID. In response to Appellant's argument that Byford does not teach a record ID, the Examiner stated, "[t]he Examiner asserts that Hoffman teaches this

feature. Byford was not used to teach a record ID.” (Office Action, 10/02/2006, page 3). Though the Examiner admits that Byford does not teach a record ID, he later states that claim 10 is unpatentable because, “Byford teaches discarding a user’s record ID.” (Office Action, 10/02/2006, page 8). Since Byford does not teach a record ID, Byford cannot teach discarding a record ID. Therefore, neither Hoffman nor Byford, alone or in combination, teach or suggest discarding a record ID.

Accordingly, Appellants respectfully request the withdrawal of the rejection over this combination.

3. Claim 25 is not obvious under 35 U.S.C. §103(a) in view of Hoffman and Byford because neither Hoffman nor Byford, alone or in combination, teach or suggest an authentication server to receive a record ID for a user.

Appellants respectfully submit that claim 25 is not obvious over the combination of Hoffman and Byford. Claim 25 depends on claim 17, and fully incorporates its limitations. Appellants respectfully submit that the combination of Hoffman and Byford does not teach or suggest an authentication server to receive a record ID for a user, as claimed in claim 17.

Byford teaches the use of biometric data for authentication. However, Byford does not teach or suggest the use of a record ID in this context. As discussed above, Hoffman does not teach or suggest receiving a record ID for a user, and Byford does not supply the missing elements.

Since neither Hoffman nor Byford, alone or in combination, teaches an authentication server to receive a record ID for a user as claimed in independent claim

17, the combination cannot be interpreted to render obvious Appellants' invention as claimed in associated claim 25.

Accordingly, Appellants respectfully request the withdrawal of the rejection over this combination.

4. Claim 28 is not obvious under 35 U.S.C. §103(a) in view of Hoffman and Byford because neither Hoffman nor Byford, alone or in combination, teach or suggest a security mechanism to discard the record ID after returning the one-time key to the user.

Appellants respectfully submit that claim 28 is not obvious over the combination of Hoffman and Byford. Claim 28 depends on claim 17, and incorporates all of its limitations, and therefore is patentable for at least the reasons discussed with reference to claim 17. Moreover, appellants respectfully submit that the combination of Hoffman and Byford does not teach or suggest a security mechanism to discard the record ID after returning the one-time key to the user, as claimed in claim 28.

Appellants respectfully submit that Hoffman in view of Byford does not teach or suggest a security mechanism to discard the record ID after returning the one-time key, the record ID being a random number generated to track the user's authentication data and used to separate the user's other identity information from the authentication data, as recited in claim 28. As discussed above with reference to claim 7, Byford does not teach a record ID, and so cannot teach discarding a record ID. The Examiner has specifically stated that Hoffman does not disclose discarding a record ID. Since neither Hoffman nor Byford, alone or in combination, teaches a security mechanism to discard

a record ID after returning a one-time key to the user, the combination cannot be interpreted to render obvious Appellants' invention as claimed in associated claims 28.

Accordingly, Appellants respectfully request the withdrawal of the rejection over this combination.

C. Claims 15, 16, 18 and 21 are not obvious under 35 U.S.C. §103(a) in view of Hoffman and U.S. Patent No. 5,692,106 to Towers et al ("Towers") because neither Hoffman nor Towers, alone or in combination, teaches or suggests each of the elements.

1. Claims 15 and 16 are not obvious under 35 U.S.C. §103(a) in view of Hoffman and Towers because neither Hoffman nor Towers, alone or in combination, teach or suggest looking up a record ID associated with a user.

Appellants respectfully submit that claims 15 and 16 are not obvious over the combination of Hoffman and Towers. Claims 15 and 16 depend on claim 14, and fully incorporate its limitations. Appellants respectfully submit that the combination of Hoffman and Towers does not teach or suggest looking up a record ID associated with a user, as claimed in claim 14.

Towers discusses the determination of authentication policy associated with a user. However, Towers does not teach or suggest the use of a record ID in this context. As discussed above, Hoffman does not teach or suggest looking up a record ID associated with a user, and Towers does not supply the missing elements. Since neither Hoffman nor Towers, alone or in combination, teaches looking up a record ID associated with a user as claimed in independent claim 14, the combination cannot be

interpreted to render obvious Appellants' invention as claimed in associated claims 15 and 16.

Accordingly, Appellants respectfully request the withdrawal of the rejection over this combination.

2. Claims 18 and 21 are not obvious under 35 U.S.C. §103(a) in view of Hoffman and Towers because neither Hoffman nor Towers, alone or in combination, teach or suggest an authentication server to receive a record ID for a user.

Appellants respectfully submit that claims 18 and 21 are not obvious over the combination of Hoffman and Towers. Claims 18 and 21 depend on claim 17, and fully incorporate its limitations. Appellants respectfully submit that the combination of Hoffman and Towers does not teach or suggest an authentication server to receive a record ID for a user, as claimed in claim 17.

As discussed above, Hoffman does not teach or suggest an authentication server to receive a record ID for a user, and Towers does not supply the missing elements. Since neither Hoffman nor Towers, alone or in combination, teaches an authentication server to receive a record ID for a user as claimed in independent claim 17, the combination cannot be interpreted to render obvious Appellants' invention as claimed in associated claims 18 and 21.

Accordingly, Appellants respectfully request the withdrawal of the rejection over this combination.

D. Claims 19 and 22 are not obvious under 35 U.S.C. §103(a) in view of Hoffman and U.S. Patent No. 6,119,227 to Mao ("Mao") because neither Hoffman

nor Mao, alone or in combination, teach or suggest a server to receive a record ID for a user.

Appellants respectfully submit that claims 19 and 22 are not obvious over the combination of Hoffman and Mao. Claims 19 and 22 depend on claim 17, and incorporate its limitations. Appellants respectfully submit that the combination of Hoffman and Mao does not teach or suggest a server to receive a record ID for a user, as claimed in claim 17.

Mao discusses nonce generation to be included with user authentication data. However, Mao does not teach or suggest the use of a record ID in this context. Mao does not discuss record IDs, and thus is silent about a record ID being a random number generated for tracking authentication data and disassociating the authentication data from other client identity data, as recited in claim 17.

As discussed above, Hoffman does not teach or suggest a server to receive a record ID for a user, and Mao does not supply the missing elements. Since neither Hoffman nor Mao, alone or in combination, teaches a server to receive a record ID for a user as claimed in independent claim 17, the combination cannot be interpreted to render obvious Appellants' invention as claimed in associated claims 19 and 22.

Accordingly, Appellants respectfully request the withdrawal of the rejection over this combination.

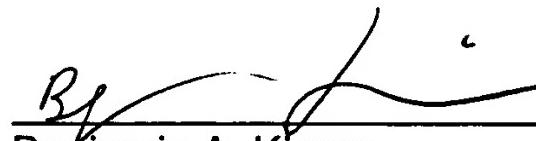
VIII. CONCLUSION

Based on the foregoing, Appellants respectfully submit that that the Board should reverse the rejection of all pending claims and hold that all of the claims currently under review are allowable.

Respectfully submitted,

BLAKELY SOKOLOFF TAYLOR & ZAFMAN

Dated: February 5, 2007



Benjamin A. Kimes
Reg. No. 50,870

IX. CLAIMS APPENDIX

The claims involved in this appeal are presented below.

1. (Previously Presented) A method of authenticating a client, the method comprising in an authentication server:
 - receiving a record ID for a user, the record ID being a random number generated for tracking authentication data and disassociating the authentication data from other client identity data, and a one-time key generated by a third party server and encrypted with a user's public key by the server;
 - receiving the user's authentication data from the client;
 - determining if the user's authentication data matches the record ID; and
 - if so, decrypting the one-time key with the user's private key, and returning the decrypted one-time key to the client.
2. (Previously Presented) The method of claim 1, further comprising registering the user with the authentication server, registering comprising:
 - receiving a registration authentication data from the user;
 - generating a random public key/private key pair for the user;
 - generating a random number as the record ID for the user; and
 - associating the authentication data and the private key with the record ID.
3. (Original) The method of claim 2, further comprising:
 - sending the record ID and the public key to the user.
4. (Previously Presented) The method of claim 2 further comprising establishing a secure connection between the authentication server and the user, prior to receiving registration authentication data.

5. (Previously Presented) The method of claim 1, wherein a web page presented by the third party server to the client prompts the user to enter the authentication data to log in to the server.
6. (Original) The method of claim 5, wherein the client's authentication data is automatically redirected to the authentication server.
7. (Original) The method of claim 1, wherein the authentication data is biometric data.
8. (Original) The method of claim 1, wherein the authentication data is personal data selected from among the following: a password, a smart card, and another type of authentication card.
9. (Previously Presented) The method of claim 1, wherein the client forwards the decrypted one-time key to the third party server, thereby authenticating the user as the owner of the private key.
10. (Original) A method of claim 1, further comprising discarding the record ID after returning the one-time key to the user.
11. (Original) The method of claim 1, wherein the record ID and the encrypted one-time key are further encrypted using a partner key, the method further comprising decrypting the record ID and encrypted one-time key using the partner key.

12. (Original) The method of claim 11, wherein the partner is a symmetric key set up during registration of the partner.

13. (Original) The method of claim 11, wherein the partner key is a private key of the authentication server.

14. (Previously Presented) A method of using an authentication server to authenticate a user to a third party server, the method comprising the third party server:

looking up a record ID associated with the user, the record ID being a random number generated to track the user's authentication data and used to separate the user's other identity information from the authentication data;

generating one-time key and encrypting the one-time key with a public key of the user, and sending the encrypted one-time key and the record ID to the user;

receiving the authentication data, the authentication data being the decrypted one-time key decrypted with the user's private key by the authentication server, such that the user does not have control of the user's private key at any time; and

permitting access to the server.

15. (Original) The method of claim 14, comprising:

determining an authentication policy associated with the user; and

verifying that the authentication policy has been satisfied, prior to permitting access to the server.

16. (Original) The method of claim 15, wherein verifying that the authentication policy has been satisfied comprises:

determining if the server should verify additional data; and

if so, requesting additional data from the user prior to generating the one-time key.

17. (Previously Presented) A third-party authentication system comprising:
an authentication server to receive a record ID for a user, the record ID being a randomly generated number used to separate the user's other identity information from the user's authentication data, and a one-time key generated by a third party server and encrypted with a user's public key by the third party server;

a comparison logic in the authentication server to receive user authentication data from the client and determine whether the user's authentication data matches the record ID; and

a decryption logic in the authentication server to decrypt the one-time key with a private key associated with the validated record ID, and to return the decrypted one-time key to the client.

18. (Previously Presented) The system of claim 17, further comprising:
a policy validation logic to receive a policy from the third party server, and determine if the policy has been fulfilled; and
the decryption logic to decrypt the one-time key only if the policy has been fulfilled.

19. (Original) The system of claim 17, further comprising:
a nonce generation logic to generate a nonce, the nonce to be included with the user authentication data from the client; and
the comparison logic to verify that the user authentication data includes the appropriate nonce.

20. (Original) The system of claim 17, further comprising a client registration logic to register the user, the client registration logic comprising:
a key generation logic to generate a random public key/private key pair for the user;
a record ID generation logic to generate a random record ID for the user; and
the client registration logic to associate user authentication data with the private key and the record ID.
21. (Original) The system of claim 18, further comprising:
the interface to send the record ID and the public key to the user.
22. (Original) The system of claim 19, wherein the interface establish a secure connection with the user, prior to receiving registration authentication data.
23. (Original) The system of claim 17, wherein a web page presented by the server to the client prompts the user to enter the authentication data to log in to the server.
24. (Original) The system of claim 23, wherein the client's authentication data is automatically redirected to the authentication server.
25. (Original) The system of claim 17, wherein the authentication data is biometric data.

26. (Original) The system of claim 17, wherein the authentication data is personal data selected from among the following: a password, a smart card, and another type of authentication card.
27. (Original) The system of claim 17, wherein the client forwards the decrypted one-time key to the server, thereby authenticating the user as the owner of the private key.
28. (Original) The system of claim 17, further comprising a security mechanism to discard the record ID after returning the one-time key to the user.
29. (Original) The system of claim 17, wherein the decryption logic further decrypts the record ID and the encrypted one-time key with a partner key.
30. (Original) The system of claim 29, wherein the partner key is a symmetric key set up during registration of the partner.
31. (Original) The system of claim 29, wherein the partner key is a private key of the authentication server.

X. EVIDENCE APPENDIX

No other evidence is submitted in connection with this appeal.

XI. RELATED PROCEEDINGS APPENDIX

No related proceedings exist.